REMARKS

Claims 1-20 are pending in the above-identified application.

The Office Action mailed December 27, 2007 (hereinafter "Office Action"), rejected Claims 1-20 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,167,988, to Hayashi et al. (hereinafter "Hayashi") and further in view of U.S. Patent No. 7,188,369, to Ho et al. (hereinafter "Ho"). Applicants respectfully disagree and submit that Claims 1-20 are not obvious over Hayashi in view of Ho because the prior arts fail to teach or suggest certain elements of both the independent and dependent claims, which are discussed in detail later in this response. While applicants disagree with the grounds of rejection cited in the Office Action, in order to advance the prosecution of the present application, Claim 2 has been slightly amended to clarify the claim language.

Pursuant to 37 C.F.R. § 1.111, and for the reasons set forth below, applicants respectfully request reconsideration and allowance of the pending claims. Prior to presenting the reasons why the applicants believe that the pending claims are in condition for allowance, a brief summary of the disclosed subject matter and brief descriptions of the teachings of the cited references are provided. These summaries, however, are presented solely to assist the Examiner in recognizing the differences between the pending claims and the cited references and should not be construed as limiting on the disclosed subject matter.

Disclosed Subject Matter

The present application discloses systems and methods for detecting malware among executable scripts. Unlike executable code, scripts are typically executed in an interpretive environment and are not compiled down to source code. Moreover, scripts are typically editable using a variety of word processing programs. Since scripts are interpreted (instead of compiled) they can be easily yet superficially modified without changing the underlying instruction. For

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

example, a variable "vName" could easily be renamed "xyzzy" throughout the body of a script without changing the functionality of the script in the least.

Malware is often detected by generating a hash of a document and checking the hash against those of known malware. In order to ensure that a legitimate file is not mistakenly identified as malware, a typical hash generation process is highly sensitive to the actual contents of the document. Unfortunately, malware designers are aware of this and have turned to modifying their malware in superficial manners to avoid detection. As indicated above, scripts can be easily modified, modified to a great degree, without changing the underlying functionality. To resolve this, the present application discloses a normalization process that generates a normalized signature for a given script and compares the normalized signature against similarly normalized signatures of known malware to determine whether the given script is malware.

The normalization process takes tokens from a script and translates them into normalized tokens according to a common naming format. For example, as recited in the specification, the variable "vName" may be translated to "V1." Routines are similarly translated to a common naming format. Additionally, non-functional statements, sometimes called no-op statements, are eliminated from the normalized signature.

When an ideal match between a normalized signature for a given script and the normalized signatures in the malware signature store is not found, a second normalized signature is generated. This second normalizing process recognizes that some statements within a script can be reordered without modifying the underlying functionality of the script. The second normalizing and comparison step addresses this. The second normalized signature removes ordinal values from the normalized tokens. For example, a first normalized token "V1" would be twice normalized simply to "V." Routine tokens are also similarly twice normalized. The result

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

(such as shown in FIGURE 11) is a significantly simplified set of tokens which form the second normalized signature. The second normalized signature is then compared to twice normalized signatures of known malware. If a complete match is found on the second normalized signature, the script is reported as being malware. If a partial match is found, a report is made that the script may be malware – leaving it to the user to determine additional actions to be taken, if any.

Hayashi

Hayashi purportedly discloses an information processing apparatus where code stream and data indicating a normalization method are inputted to a normalization processing unit, and the normalization processing unit applies normalization processing to the code stream to generate a normalized code stream. Next, when signature data is inputted, a verification processing unit performs encryption and decryption processing with respect to the signature data using a public key and calculates a Hash value (first Hash value) and, on the other hand, calculates a Hash value of the normalized code stream (second Hash value). Next, the verification processing unit compares the first Hash value and the second Hash value and, if the first Hash value and the second Hash value are equal, judges that the code stream is not falsified. On the other hand, if the first Hash value and the second Hash value are not equal, the verification processing unit judges that the code stream is falsified.

While Hayashi purportedly discloses a normalization processing unit that takes as input a code stream and data indicating a normalization method to output a normalized code stream, Hayashi fails to disclose normalizing script (as disclosed by the present application) to generate normalized signatures and comparing a normalized signature to similarly normalized signatures of known malware to determine whether the code stream is malware.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682 8100

Ho

Ho purportedly discloses an antivirus system having a virtual processor and plug-in capabilities. The Ho system includes an antivirus database having signatures of known viruses. The processor can receive instructions external to the system for execution in scanning for viruses. Using the signatures and the internal and external instructions, the Ho system scans files (including generating signatures and comparing those signatures to known virus signatures in the antivirus database) to determine whether the files are/contain viruses.

While Ho purportedly discloses a particular antivirus system and suggests that viruses may be identified by their signatures, Ho fails to disclose normalizing script (as disclosed by the present application) to generate normalized signatures and comparing a normalized signature to similarly normalized signatures of known malware.

35 U.S.C. § 103(a) Rejections

As noted above, the Office Action rejected Claims 1-20 under 35 U.S.C. § 103(a) as being unpatentable over Hayashi and further in view of Ho. Applicants respectfully disagree. While applicants disagree with the grounds of rejection cited in the Office Action, in order to advance the prosecution of the present application, Claim 2 has been slightly amended to clarify the claim language.

Claim 1

Applicants submit that Hayashi and Ho, alone or in combination, fail to disclose the following elements as recited in Claim 1:

> a malware signature store including at least one known malware script signature, wherein each malware signature in the malware signature stored is a normalized signature of a known malware script; and
>
> a normalization module that obtains an executable script and generates a normalized signature for the executable script, wherein generating a normalized signature for the executable script comprises translating tokens

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

from the executable script into normalized tokens conforming to a common format;

wherein the malware detection system is configured to:
compare the normalized signature of the executable script to the at least one normalized malware signature in the malware signature store to determine whether the executable script is malware.

Applicants agree that Hayashi does not explicitly teach a malware signature store. Accordingly, Hayashi fails to teach "a malware signature store including at least one known malware script signature, wherein each malware signature in the malware signature stored is a normalized signature of a known malware script."

The Office Action asserts that Hayashi teaches a normalization module that obtains an executable script and generates a normalized signature for the executable script, wherein generating a normalized signature for the executable script comprises translating tokens from the executable script into normalized tokens conforming to a common format at Col. 8, lines 1-9. Applicants respectfully disagree. The aforementioned section of Hayashi purportedly discloses that normalized code stream outputted from a normalization processing unit is inputted to a signature processing unit, and the signature processing unit generates signature data using a public key cryptosystem. Firstly, nowhere does Hayashi teach, explicitly or implicitly, that the generated signature data is normalized. Secondly, nowhere does Hayashi teach, explicitly or implicitly, that the generated signature data is created by translating tokens from the code stream into normalized tokens conforming to a common format. In fact, Hayashi explicitly teaches at Col. 7, lines 39-52, that the normalization method adopted by the normalization module includes various compression coding parameters. However, Hayashi also explicitly teaches that the normalization method is not limited to include various compression coding parameters and, for example, it is also possible to determine several normalization methods in which various compression coding parameters are written as classes in advance. In the example where various compression coding parameters are written as classes in advance, a normalization method is

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

determined as a class and contents of the class is shared by the signature processing unit and a verification processing unit of a verification device whereby it is sufficient to send an identifier, which indicates the class from the signature processing unit to the verification processing unit of the verification device. In contrast, the normalization method of the present invention translates tokens from an inputted executable script into normalized tokens conforming to a common format. Accordingly, Hayashi does not teach "a normalization module that obtains an executable script and generates a normalized signature for the executable script, wherein generating a normalized signature for the executable script comprises translating tokens from the executable script into normalized tokens conforming to a common format."

The Office Action asserts that Hayashi teaches wherein the malware detection system is configured to compare the normalized signature of the executable script to the at least one normalized malware signature in the malware signature store to determine whether the executable script is malware at lines 10-16 of the Abstract. Applicants respectfully disagree. The aforementioned section of Hayashi purportedly teaches calculating a first Hash value using a public key and a second Hash value of the normalized code stream, and comparing the first Hash value and the second Hash value. Firstly, as noted above, Hayashi fails to teach, explicitly or implicitly, that the generated signature is normalized. Secondly, nowhere does Hayashi teach a malware detection system, let alone a malware detection system that is configured to determine whether an executable script is malware. Thirdly, and as noted above, applicants agree with the Office Action remarks that Hayashi fails to teach a malware signature store. Accordingly, Hayashi does not teach "wherein the malware detection system is configured to compare the normalized signature of the executable script to the at least one normalized malware signature in the malware signature store to determine whether the executable script is malware."

As explained above, Hayashi fails to teach or suggest a computer-implemented malware detection system for determining whether an executable script is malware according to its functionality because Hayashi fails to teach or suggest "a malware signature store including at least one known malware script signature, wherein each malware signature in the malware signature stored is a normalized signature of a known malware script," "a normalization module that obtains an executable script and generates a normalized signature for the executable script, wherein generating a normalized signature for the executable script comprises translating tokens from the executable script into normalized tokens conforming to a common format," and "wherein the malware detection system is configured to compare the normalized signature of the executable script to the at least one normalized malware signature in the malware signature store to determine whether the executable script is malware."

While Ho describes an antivirus database that holds a plurality of virus signatures, nothing in Ho describes or suggests that the signatures in the database have been normalized, i.e., where tokens are translated to a common naming structure suitable for comparison to other normalized signatures. This is especially the case as the claim itself recites that generating a normalized signature "comprises translating tokens from the executable script into normalized tokens conforming to a common format." As recited above, normalizing tokens in a script enable the system to compare the underlying structure of a script to normalized signatures (underlying structure) of known malware, looking beyond superficial renaming of tokens. Applicants submit that Ho, like Hayashi, also fails to disclose such normalized signatures, as well as normalizing the script for comparison to normalized signatures of known malware.

Whether or not Hayashi and Ho are properly combined, Hayashi and Ho do not teach, suggest, or describe the foregoing aspects of the invention recited in Claim 1. Generally described, under 35 U.S.C. § 103(a), a *prima facie* case of obviousness can be established only if

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

the cited references, alone or in combination, teach each and every element recited in the claim. *In re Bell*, 991 F2d 781 (Fed. Cir. 1993). Hayashi and Ho, alone or in combination, fail to teach or suggest "a malware signature store including at least one known malware script signature, wherein each malware signature in the malware signature stored is a normalized signature of a known malware script," "a normalization module that obtains an executable script and generates a normalized signature for the executable script, wherein generating a normalized signature for the executable script comprises translating tokens from the executable script into normalized tokens conforming to a common format," and "wherein the malware detection system is configured to compare the normalized signature of the executable script to the at least one normalized malware signature in the malware signature store to determine whether the executable script is malware." Accordingly, applicants respectfully request withdrawal of the pending rejection under 35 U.S.C. § 103(a) with regard to Claim 1, and the allowance of Claim 1.

Claim 2

Applicants submit that since Claim 2 depends from Claim 1, Claim 2 is allowable for the same reasons as set forth above. Accordingly, applicants request that the 35 U.S.C. § 103(a) rejection of Claim 2 be withdrawn and the claim allowed.

Claims 3-5

While differing in scope, applicants point out that independent Claims 3-5 recite similar subject matter to that described in independent Claim 1. In particular, Claim 3 recites:

> a malware signature storage means including at least one known malware signature, wherein each malware signature in the malware signature store means is a normalized signature of a known malware script;
>
> a normalization means that obtains an executable script and generates a normalized signature for the executable script, wherein the normalized signature for the executable script comprises a set of normalized tokens

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

translated from corresponding tokens in the executable script into a common format suitable for comparison with the at least one malware signature in the malware signature store means; and

a comparison means that compares the normalized signature for the executable script to the at least one malware signature in the malware signature storage means.

Claim 4 recites:

generating a first normalized signature for the executable script, wherein the first normalized signature comprises normalized tokens translated from corresponding tokens in the executable script in a format suitable for comparison to normalized signatures of known malware;

comparing the first normalized signature to at least one normalized signature of known malware; and

determining, based on the previous comparison, whether the executable script is malware.

Claim 5 recites:

generating a first normalized signature for the executable script, wherein the first normalized signature comprises normalized tokens translated from corresponding functional contents of the executable script in a format suitable for comparison to normalized signatures of know malware;

comparing the first normalized signature to at least one normalized signature of known malware scripts; and

determining, based on the previous comparison, whether the executable script is malware.

As can be seen from above, these independent claims recite elements that are not taught or suggested, alone or in combination, by Hayashi and Ho. Accordingly, applicants request that the 35 U.S.C. § 103(a) rejections of Claims 3-5 be withdrawn and the claims allowed.

Claims 6-9

Applicants submit that since Claims 6-9 depend directly or indirectly from Claim 1, Claims 6-9 are allowable for the same reasons as set forth above. Accordingly, applicants

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682.8100

request that the 35 U.S.C. § 103(a) rejections of Claims 6-9 be withdrawn and the claims allowed.

Claims 10-12

Applicants submit that since Claims 10-12 depend directly or indirectly from Claim 3, Claims 10-12 are allowable for the same reasons as set forth above. Accordingly, applicants request that the 35 U.S.C. § 103(a) rejections of Claims 10-12 be withdrawn and the claims allowed.

Claims 13-16

Applicants submit that since Claims 13-16 depend directly or indirectly from Claim 4, Claims 13-16 are allowable for the same reasons as set forth above. Accordingly, applicants request that the 35 U.S.C. § 103(a) rejections of Claims 13-16 be withdrawn and the claims allowed.

Claims 17-20

Applicants submit that since Claims 17-20 depend directly or indirectly from Claim 5, Claims 17-20 are allowable for the same reasons as set forth above. Accordingly, applicants request that the 35 U.S.C. § 103(a) rejections of Claims 17-20 be withdrawn and the claims allowed.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

CONCLUSION

In view of the above remarks, applicants respectfully submit that the present application is in condition for allowance. Reconsideration and reexamination of the application, and allowance of the claims at an early date, are solicited. If the Examiner has any questions or comments concerning the foregoing response, the Examiner is invited to contact the applicants' undersigned attorney at the number below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}

Clint J. Feekes
Registration No. 51,670
Direct Dial No. 206.695.1633

CJF:jlg

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100